FUNDAÇÃO CENTRO DE ANÁLISE, PESQUISA E INOVAÇÃO TECNOLÓGICA
CENTRO DE PÓS-GRADUAÇÃO E EXTENSÃO FUCAPI – CPGE

Segurança em camadas

Fundamentos de Segurança da Informação

Conceito

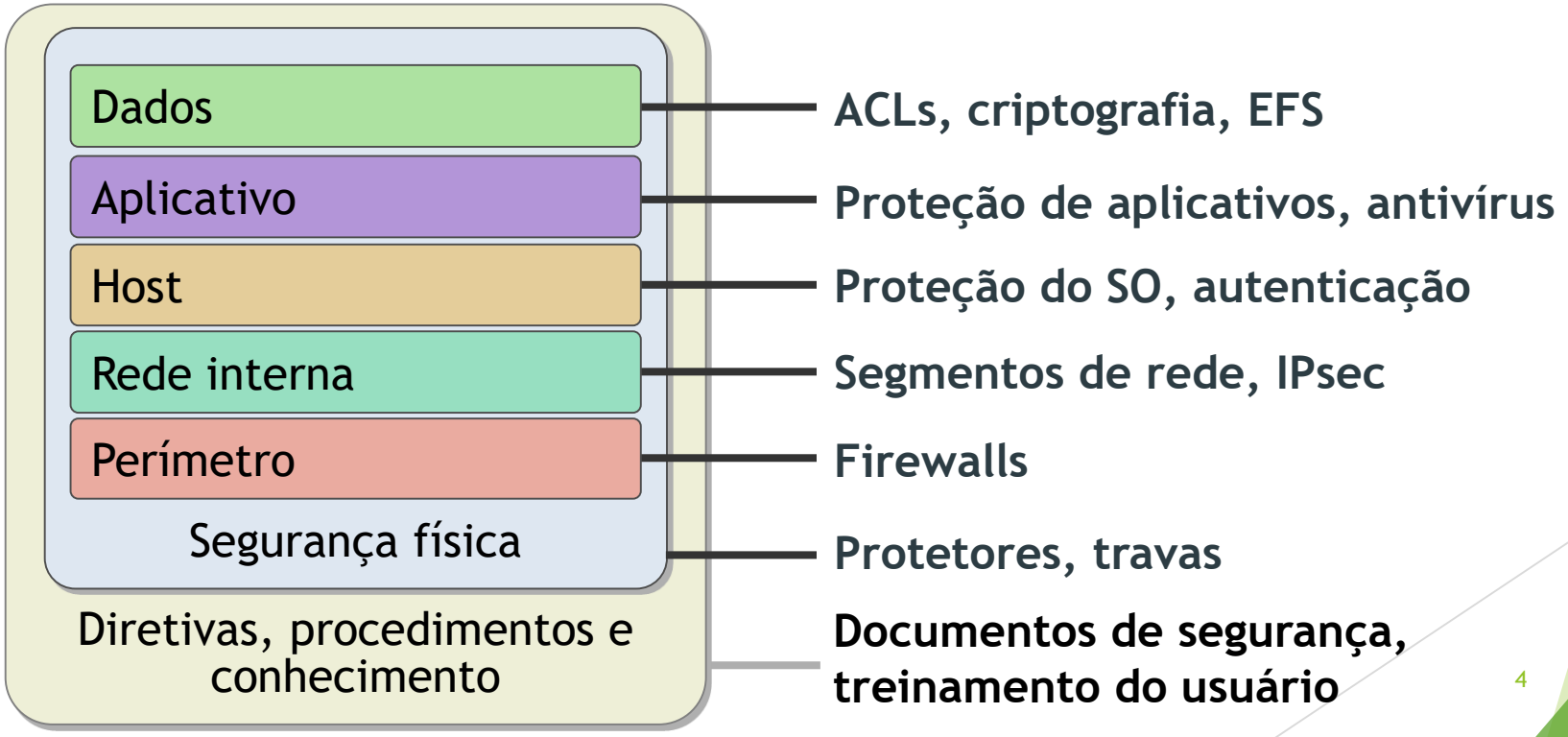
- Segurança em camadas (defense-in-depth)
  - Ao descobrir e documentar os riscos que sua organização corre, a próxima etapa é examinar e organizar as proteções que você usará para fornecer uma solução de segurança
  - O modelo de segurança de proteção em camadas é um ótimo ponto de partida para essa solução.

Conceito

- Segurança em camadas (defense-in-depth)
  - Esse modelo identifica sete níveis de segurança que devem ser abordados.
  - As camadas de proteção fornecem uma visão geral do ambiente, área por área, que deve ser levada em conta na criação de uma estratégia de segurança da rede.

Conceito

- Segurança em camadas (defense-in-depth)



Camada de dados

- Camada de dados
  - Essa camada concentra-se no acesso aos dados organizacionais, como documentos, conteúdo de banco de dados ou informações de cliente.
  - As possíveis proteções incluem permissões NTFS, permissões de banco de dados e permissões em arquivos e pastas.

Camada de dados

- Access control list (ACL)
  - Contém a lista dos usuários, grupos ou computadores que possuem acesso à um determinado recurso no domínio.
- Access control entry (ACE)
  - É cada registro de usuário, grupo ou computador dentro de uma ACL.

Camada de dados

- Permissões de arquivo
  - Permitem acesso à um determinado arquivo, seja local ou via rede, através de uma ACL e ACEs.
- Permissões de compartilhamento
  - Permitem acesso via rede à uma determinada pasta compartilhada.

Camada de dados

- Criptografia
  - É um recurso utilizado para manter em segredo as informações de um arquivo ou tráfego de rede.
- EFS
  - É um sistema que criptografa arquivos.

Camada de aplicativo

- Camada de aplicativo
  - Essa camada concentra-se nos riscos a um aplicativo em execução.
  - Em geral, trata-se de algum tipo de malware que aproveita uma vulnerabilidade em um aplicativo.
  - As possíveis proteções incluem garantir que as atualizações mais recentes sejam aplicadas aos aplicativos e reduzir o número de aplicativos, se possível.

Camada de aplicativo

- Antivirus, Antimalware, Antispyware
  - São ferramentas que mantém o computador livre de malwares, cavalos de tróia, vírus e spywares.
  - Devem ter a instalação automatizada e o gerenciamento centralizado.
  - Devem gerar relatório para análise diária.

Camada de host

- Camada de host
  - Essa camada concentra-se nos riscos ao sistema operacional e aos serviços do sistema operacional.
  - Em geral, trata-se de algum tipo de malware que aproveita uma vulnerabilidade no sistema operacional.
  - As melhores proteções limitarão os serviços somente a aqueles que são exigidos e aplicarão atualizações de segurança rapidamente.

Camada de host

- Firewall
  - É um mecanismo de proteção que controla a passagem de pacotes entre redes, tanto locais como externas.
  - É um dispositivo que possui um conjunto de regras especificando que tráfego ele permitirá ou negará.
  - É um dispositivo que permite a comunicação entre redes, de acordo com a política de segurança definida e que são utilizados quando há uma necessidade de que redes com níveis de confiança variados se comuniquem entre si.

Camada de rede interna

- Camada de rede interna
  - Essa camada concentra-se nos riscos aos dados na rede interna.
  - A principal preocupação é o acesso não autorizado aos dados enquanto estes estiverem na rede.
  - Vários métodos podem ser usados para garantir que os clientes sejam autenticados adequadamente antes de receberem acesso à rede.
  - Os dados de rede também podem ser criptografados usando o IPSec.

Camada de rede interna

- IPSec
  - O IPSec fornece diversas opções para executar a encriptação e autenticação na camada de rede.
  - Quando dois nós desejam se comunicar com segurança, eles devem determinar quais algoritmos serão usados (se DES ou IDEA, MD5 ou SHA).
  - Após escolher os algoritmos, as chaves de sessão devem ser trocadas.

Camada de rede interna

- IPSec
  - Associação de Segurança é o método utilizado pelo IPSec para lidar com todos estes detalhes de uma determinada sessão de comunicação.
  - Uma SA representa o relacionamento entre duas ou mais entidades que descreve como estas utilizarão os serviços de segurança para se comunicarem.

Camada de rede de perímetro

- Camada de rede de perímetro
  - Essa camada concentra-se nos riscos que surgem quando se acessa recursos na rede de perímetro pela Internet.
  - A configuração do firewall é o principal método de proteção dessa camada, mas outros métodos, como sistema de detecção de invasão, também podem ser usados

Camada de segurança física

- Camada de segurança física
  - Essa camada concentra-se no acesso físico a dispositivos e nos riscos associados a esse acesso.
  - Alguns riscos físicos incluem dispositivos USB com malware e inicialização de sistemas em um sistema operacional alternativo para acesso a dados.

Camada de diretivas, procedimentos e reconhecimento

- Camada de diretivas, procedimentos e reconhecimento
  - Essa camada cerca todas as outras camadas, pois afeta todas elas.
  - As políticas e os procedimentos que sua organização implementa são essenciais para prevenir riscos à segurança em cada camada.
  - Além disso, o reconhecimento desses procedimentos e políticas é necessário para garantir que eles sejam seguidos.

Dúvidas?

Contato

- alex@feleol.com.br
- http://feleol.com.br
- http://sec4all.com.br
- http://alexfeleol.com.br

Por fim...